Darktrace Enterprise

Threat Detection & Classification

The ability to detect and classify unusual behavior, as it emerges, is critical in this era of novel and fast-moving cyber-threat. Today's rapidly evolving threat landscape demands a fundamentally new approach to detecting attacks at an early stage, before they have time to do damage.

To address the challenge, organizations must understand when benign activity turns 'abnormal' amid the noise of everyday business activity, and to differentiate friend from foe. In order to do this, across a diverse and changeable digital environment, technology must be able to make judgments autonomously, and help security professionals focus on what really matters.

Enterprise Immune System

Darktrace Enterprise is Darktrace's flagship AI cyber defense solution. It combines real-time threat detection, network visualization, and advanced investigation capabilities in a single unified system that is fast and easy to install.

Using proprietary machine learning and AI algorithms developed by mathematicians from the University of Cambridge, Darktrace Enterprise detects and ranks all forms of cyber-threats, including subtle insider threats, low-and-slow attacks and automated threats, without prior assumptions of what 'malicious' activity looks like.

The solution works by passively analyzing raw network traffic across the digital enterprise, and continually makes probabilistic judgments about what is normal or abnormal behavior. In doing so, Darktrace creates an evolving understanding of the 'pattern of life' of every device and user, as well as each network and subnet.

Based on core Enterprise Immune System technology, these 'patterns of life' are dynamic, and adapt as your network evolves. Without presuming to know in advance what activity is 'malicious' or not, Darktrace Enterprise independently learns to detect significant deviations from the 'pattern of life' of a business, and immediately alerts the organization to the potential threat.

This probability-based approach means that Darktrace Enterprise is agnostic to the provenance, delivery mechanism, tactics and function of the cyber-attacker or threat. All significant deviations are seen and correlated, resulting in the detection of genuine threats, without producing floods of false positives.

Critically, Darktrace Enterprise is self-improving too, becoming increasingly accurate over time.

Key Benefits

Learns on the Job
Continually learns and adapts its understanding of 'normal' in light of new evidence.

Understands Your Entire Business
Works across on-premise network, data center, virtualized environment, cloud, SaaS, industrial control systems.

Installs in One Hour
No lengthy set-up or manual tuning. Darktrace Enterprise installs in just one hour.

> **Darktrace has proven the technology actually does what it says it will.**
>
> FORRESTER®

Network Visualization

Cyber security analysts face not only overwhelming volumes of data but also increased complexity as the digital business continues to expand. In this environment, an efficient and effective way to visualize interconnected data is essential to allow for sophisticated threat detection and remediation.

To defend their networks against a range of attack types, organizations require a powerful tool that provides insight into the relationships and data flows across the network, as well as intuitive visual storytelling that can be used to identify and investigate potential emerging threats as they unfold.

Darktrace Threat Visualizer

Darktrace Threat Visualizer

The Threat Visualizer is Darktrace's graphical and interactive 3D interface, which visualizes network activity and enables users to investigate anomalies in real time. It is designed for users of all maturity levels, from forensic security experts, to business executives and less experienced members of the IT team.

A wealth of rich information can be variously queried and exposed using the interactive features within the Threat Visualizer. Cyber security analysts use it as an essential system to investigate cyber incidents, while visualization techniques provide a high-level overview of security issues for business executives, helping to bridge the gap between technical specialists and the boardroom.

> " Darktrace has an excellent user interface and enables analysts to visualize the entire network. "
>
> **- Gartner Peer Insights Review**

Dynamic Threat Dashboard

The Dynamic Threat Dashboard provides a simplified, real-time view of high-priority threats and suspicious activities to help expedite the response process. This allows even the leanest security teams to perform extremely rapid triage with a minimum of interaction. Its streamlined interface facilitates quick sorting, viewing, and acknowledging of breaches, which can then be investigated by pivoting to the Threat Visualizer, which gives a comprehensive view of the relevant network activity.

> " The Dynamic Threat Dashboard provides focus and is extremely easy to use. "
>
> **- Gartner Peer Insights Review**

Darktrace Mobile App

Available for iOS and Android, the Darktrace Mobile App allows users to easily access Darktrace when they are on the move. Designed to offer maximum flexibility and to increase the speed of mitigation, the app offers push notifications of in-progress threats and one-click confirmation of Darktrace Antigena's autonomous response actions. When an attack transpires, security teams can remotely view and remediate threats within seconds, even when they are out of the office.

Darktrace Mobile App

> " The Darktrace Mobile App is great. It gives me the flexibility to take actions, get alerts, and monitor the network wherever I am. "
>
> **- ZPower**

Contact Us

North America: +1 (415) 229 9100

Latin America: +55 (11) 97242 2011

Europe: +44 (0) 1223 394 100

Asia Pacific: +65 6804 5010

info@darktrace.com